An Extended Identity Based Authenticated Asymmetric Group Key Agreement Protocol

Reddi Siva Ranjani, D. Lalitha Bhaskari, P. S. Avadhani
(Corresponding author: Reddi Siva Ranjani)

Department of Computer Science and Systems Engineering, Andhra University
Visakhapatnam, Andhra pradesh, India.
(Email: rsivaranjani552008@gmail.com)

(Received Sept. 29, 2013; revised and accepted Feb. 18 & Mar. 13, 2014)

Abstract

Lei et al. [26] proposed a new asymmetric group key agreement protocol allowing a set of users to negotiate a common encryption key accessible by any user, and each user holds her respective decryption key. This enables the confidential message communication among group users, and grants any outsider to send message to the group. In this paper, an authenticated asymmetric group key agreement protocol is proposed, which offers security against active as well as passive attacks. Proposed protocol uses broadcast encryption mechanism without relying on the trusted dealer to distribute the secret key. An identity based feature is included in the protocol to provide authentication.

Keywords: Identity based, group key agreement, pairings, public key cryptography

1 Introduction

Group Key Agreement (GKA) Protocols [1, 14] allow a group of users to derive a common secret key, from which a session key can be inferred. Therefore, they are used in any group oriented communication applications, such as video conference, priced VCD distribution and collaborative computations. All these applications require secure broadcasting at the network layer among the parties in the group communication. In conventional group key agreement, all the users in the group establish a common shared secret key, which is used in message encryption and decryption. In the recently developed asymmetric key agreement protocol by Wu et al. [23], all the group participants negotiate a common encryption key which is accessible to all including non group members, unlike the regular GKA. Each group participant holds his own contribution, which is used in his secret decryption key derivation. Therefore, beside the group participants, Asymmetric Group Key Agreement Protocols (AGKAP) allows outsiders of the group to broadcast the cipher messages to the group participants, provided that the sender knows the negotiated public key.

1.1 Motivation and Contributions

Group key management protocols [19, 22] are classified into group key distribution protocols and group key agreement protocols. The group key distribution protocols [2] are used to distribute group key to the group participants. In group key agreement, group participants are actively involved in the derivation of group key. Compared with conventional group key agreement protocol, AGKAP is having the advantage of one round efficiency. Many of the popular conventional GKA protocols require two or more rounds for sharing the common secret key. In these protocols, all the participants should be connected concurrently in order to share the key. However, if the participants are located in different locations with different time zones, it is very difficult for them to be connected concurrently. But, single round ASGKA protocols [17, 23] have several advantages over the GKA protocols with two or more rounds. The single round ASGKA allows each participant to publish their public key contribution by holding their respective secret key. The participant need not be connected during the key sharing. To send a message to participants in the group, the sender encrypts the message commonly using the derived common group public key and generates the cipher text. The protocols developed are efficient but secure against passive attacks only. However, in real world attackers are active attackers, who can control the communication channel to place powerful attacks. Man-in-middle attack and also, with which the active attackers can delay, modify, replay and insert the messages during the execution of the protocol. Hence, it is imperative for an ASGKA protocol to resist against the attacks from active adversaries.

Any Authenticated key agreement protocol [9, 10, 15, 20, 27], which ensures that no entities other than intended participant can possibly compute the agreed group session key, even the attacker is active or passive. In authenticated key agreement protocols, each user can obtain others certificate, extract other participant's public key, checks the validity of the certificate and then finally a common group key was computed. Consequently, the management of the certificate incurs overheads computation, storage and communication. To eliminate such overhead costs, Identity Based Public Key Cryptography (IB-PKC) that was introduced by Shamir [21]. The distinct feature of IBPKC is that the public key is derived using the participant identity such as telephone number and email-ID. The corresponding private key is derived only by the trusted third party, Private Key Generator (PKG) who owns the master secret of the system.

In this paper, a security model for identity based authenticated asymmetric group key agreement protocol is developed. Our protocol is based on the identity based batch multi signature with batch verification [8, 25] to generate identity based signature. Furthermore, participant identity is used in the derivation of broadcast message computations. The proposed protocol is like an authenticated group key agreement protocol with following features:

- Permits the group having any number of members without compromising the security.
- Facilitates the mutual authentication between the Group Controller and members in the group.
- Performance is compared with existing protocols.
- Allows users to broadcast public information by concealing private information. A Common group key is inferred from public information, which is received from other group members.

1.2 Related Works

Firstly, Diffie and Hellman [12] proposed a solution to key agreement; later Joux [17] extended the key agreement to three parties. Many attempts have been performed to extend the Diffie-Hellman and Joux protocols to n participants. Burmester-Desmedt [7] protocol succeeded in extending the key agreement protocol with two rounds and irrespective on participants' count. For key agreement protocols in open networks, communication should be secure against active adversaries. But, Diffie- Hellman, Joux and Burmester-Desmedt protocols do not authenticate the communicating entities.

To add authentication, several protocols have been proposed among them, the GKA protocol [16, 18] is based on IBPKC, which refers to Katz and Yung's result [11] for an authenticated version. Bresson et al. [5] formalized the first security model for group key agreement protocol, extending the group key agreement between two or three parties. Subsequently, the model was refined and modified by Bresson et al. [4, 6]. Later Lei et al. [24] extended these models to define the security of IB-AAGKA protocol, later it was extended to broadcast encryption application for open networks [26]. In this paper, we extended these models to define identity based asymmetric asynchronous group key agreement protocol.

1.3 Paper Outline

Section 2, reviews of Bilinear maps and some complexity assumptions were discussed. Section 3 defines the proposed protocol, security issues of the proposed protocol are discussed in Section 4, Section 5 discusses whole about the performance evaluation and finally we concluded the work in Section 6.

2 Preliminaries

In this section, we put forward the notations, definitions that we used in the discussion of the forth coming sections.

Bilinear Maps. We review the basic notations of the bilinear maps [3, 25] under our proposal. Let $(G_1, +)$ and $(G_T, *)$ be two groups of prime order $q > 2k$ for a security parameter $k \in N$. A function $e\colon G_1 \times G_1 \longrightarrow G_T$ is said to be a bilinear map if it satisfies the following properties:

1) Bilinearity:

$$\begin{aligned} e(aP, bQ) &= e(P,Q)^{ab}, \forall P,Q \in G_1; a,b \in Z. \\ e(P+Q,R) &= e(P,R) * e(Q,R) \\ e(P,Q+R) &= e(P,Q) * e(P,R), \forall P,Q,R \in G_1. \end{aligned}$$

2) Non-degeneracy: $e(P,Q) = 1; iff \quad P = 1$.

3) Computability: There exists a polynomial time algorithm to compute $e(P,Q), \forall P,Q \in G_1$.

A bilinear map is defined as a probabilistic polynomial time algorithm (E) that takes a security parameter k and returns a uniformly random tuple (G_1, G_T, e, g, q) of bilinear parameters, where g is the generator of G_1 and e is the bilinear map.

Consequences of Pairings. Pairings have important consequences on the hardness of certain variants of the Diffie-Hellman problem. For instance, symmetric pairings lead to a strict separation between the intractability of the Computational Diffie-Hellman problem and the hardness of the corresponding decision problem. The security of our proposal is based on the hardness of the computational Diffie-Hellman (CDH) problem, Divisible computational Diffie-Hellman and K-Bilinear Diffie-Hellman exponent, which are described below:

- Computational Diffie-Hellman (CDH): Given g, g^α, g^β for unknown $\alpha, \beta \in Z_q$, compute $g^{\alpha\beta}$.
- CDH Assumption: The assumption states that Adv[E] cannot be negligible for any polynomial time algorithm E, where $Adv[E] = Pr[E(g, g^\alpha, g^\beta) = g^{\alpha\beta}]$ and Pr describes the probability.

- Divisible Computational Diffie-Hellman (DCDH) Problem: Given g^{α}, g^{β} for unknown α, $\beta \in Z_q$, compute $g^{\alpha/\beta}$.
- DCDH Assumption: There is no polynomial time algorithm that can solve the DCDH problem with the non negligible property.
- k-Bilinear Diffie-Hellman Exponent ($k - BDHE$) Problem: Given g, h, and $y_i = g^{\alpha^i}$ in G_1 for $i = 1, 2, \cdots, k, k+2, \cdots, 2k$ as the input and compute $e(g,h)^{\alpha^{k+1}}$. Since the input vector lacks $g^{\alpha^{k+1}}$ term, the bilinear map does not seem to help to compute $e(g,h)^{\alpha^{k+1}}$.
- k-BDHE Assumption: Let E be an algorithm which has an advantage in solving k-BDHE problem. There is no polynomial-time algorithm that can solve the k-BDHE problem with non-negligible probability.

$$\begin{aligned} Adv[E] &= Pr[E(g,h,y_1,y_2,\cdots,y_k, \\ &\qquad y_{k+2},\cdots,y_{2k},e(g,h)^{\alpha^{k+1}})]. \end{aligned}$$

3 Our Proposal

In this section, we proposed the identity based asymmetric group key agreement protocol based on [23, 26]. We considered a group of n participants who are intended to receive secure messages from the participants, who may or may not be the group participants. Our scheme adopts bilinear pairings; it can be organized in terms of following stages. The algorithm works as follows:

Setup. The group Controller (U_0) generates the system parameters in this stage. The U_0 generates a uniformly tuple $P = (G_1, G_T, e, H, g, q)$ of bilinear instance. U_0 chooses a cryptographic hash function $H : \{0,1\}^* \longrightarrow G_1$, where G_1 be the group with prime order q, $e : G_1 X G_1 \longrightarrow G_T$ is a bilinear map and g is the generator of G_1. Also generate and propagate securely the private (s_i) and public keys ($Ppub_i$) to each user.

Key Establishment. At this stage, the participants in the group communication generate and publish the messages which will be used in the generation of group encryption and decryption keys. Let $U_1, U_2, U_3, \cdots, U_n$ be the participants involved in the group communication. Each participant U_i with identity ID_i for $1 \leq i \leq n$ in group communication will perform the following steps.

1) Randomly choose $h_i \in G_1, r_i \in Z_q^*$ and compute $x_i = g^{r_i}$, $A_i = e(H(ID_i) + h_i, g)$.
2) For $1 \leq j \leq n$, compute $\sigma_{i,j} = h_i * H(ID_j)^{r_i}$.
3) Generate a signature ρ_i on x_i using s_i. In order to keep the protocol efficient, one may choose the an identity based signature scheme, which provides the batch verification to generate ρ_i.
4) Publish $\{\sigma_{i,1}, \cdots, \sigma_{i,i-1}, \sigma_{i,i+1}, \cdots, \sigma_{i,n}, (x_i, A_i, ID_i, \rho_i)\}$.

After completion of this stage, each participant can get the messages as shown in the table 1, where $\sigma_{i,i} = h_i * H(ID_i)^{r_i}$ is not be published to any other user in the group communication, but it is kept secret by U_i.

Encryption Key Derivation. Any user in the group can compute the group encryption key (W, A, Q), where

$$\begin{aligned} W &= \Pi_{i=1}^{n} x_i \\ A &= \Pi_{i=1}^{n} A_i \\ Q &= \Pi_{i=1}^{n} H(ID_i). \end{aligned}$$

The group encryption key (W, A, Q) is accepted if all the n message signatures pairs $(x_1, \rho_1), (x_2, \rho_2), \cdots, (x_n, \rho_n)$ are valid.

Decryption Key Derivation. The user U_i computes the individual decryption key $d_i = \Pi_{l=1}^{n} \sigma_{l,i}$ and accepts the d_i if all the n message signatures pairs $(x_1, \rho_1), (x_2, \rho_2), \cdots, (x_n, \rho_n)$ are valid.

Encrypt. After knowing the public parameters generated by U_0, and the group encryption key (W, A, Q), any user U_i in the group communication can encrypt any message m by executing following steps.

1) Select a random number $t \in Z_q$.
2) Compute the variables $C_1 = g^t$, $C_2 = W^t$ and $C_3 = m * A^t$.
3) Communicate the cipher text $C = (C_1, C_2, C_3)$ to the receiver.

Decrypt. To deduce the plaintext from the cipher text, each participant U_i can decrypt

$$m = \frac{C_3}{e(d_i, C_1) * e(Q, C_1) * e(H(ID_j)^{-1}, C_2)} \qquad (1)$$

4 Security Analysis

Our proposed protocol is equipped with all the following security attributes.

1) Known Key Security: For each session, the participant randomly selects h_i and r_i, results separate independent group encryption and decryption keys for other sessions. Therefore, a leakage of group decryption keys in one session will not help in the derivation of other session group decryption keys.

2) Unknown Key Share: In our protocol, each participant U_i should generate a signature ρ_i using x_i. Therefore, only group participants can verify whether the coming ρ_i is from authorized person or not. Hence, no non group participant can be impersonated.

Table 1: Message obtained by the participants

User	U_1	U_2	U_3	$\ldots$	U_n	All
U_1	–	$\sigma_{1,2}$	$\sigma_{1,3}$	$\ldots$	$\sigma_{1,n}$	(x_1, A_1, ID_1, ρ_1)
U_2	$\sigma_{2,1}$	–	$\sigma_{2,3}$	$\ldots$	$\sigma_{2,n}$	(x_2, A_2, ID_2, ρ_2)
U_3	$\sigma_{3,1}$	$\sigma_{3,2}$	–	$\ldots$	$\sigma_{3,n}$	(x_3, A_3, ID_3, ρ_3)
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
U_n	$\sigma_{n,1}$	$\sigma_{n,2}$	$\sigma_{n,3}$	$\ldots$	–	(x_n, A_n, ID_n, ρ_n)

Table 2: Comparison with various protocols

	[13]	[18]	[26]	Our Protocol
Exponentiation	3	3	0	0
Multiplications	2n-2	$n^2/2 + 3n/2 - 3$	Sender: 2n Reciever: 2n	Sender: 2n Reciever: 2n
Verification or Comparisons	n+1	2n-2	n: sender n-1: participants	n-1:participants
No. of Rounds	2	3	1	1

3) Key Compromise Impersonate: Due to generation of unforgeable signature by the user U_i, the adversary cannot generate the valid signature on behalf of U_i. Even if the participant U_j's private key is compromised by the adversary, he cannot impersonate other participant U_i with U_j's private key. Hence, key impersonation property is not possible in the proposed protocol.

5 Performance Evaluation

In this section we are summarizing the performance of the proposed protocol and two other authenticated asymmetric group key agreement protocols under the same cryptosystem setting. Table 1 shows message obtained by the participants.

Round Efficiency. To constitute a session key, the existing Group Key Agreement (GKA) protocols [13, 18] requires two or more rounds, Therefore, all the participants in these protocols should connect concurrently. As in [26], our protocol, each participant needs to transmit message only once. Although both require only one round, we achieved a stronger security against active attacks. In the one round feature each participant can simply send the intermediate value and leave.

Computational Overhead. As to the computational overhead our protocol is same as the protocol [26] at the key Agreement, Encryption and Decryption, but ours not require any certificate. At the Encryption and decryption sides the computational overheads are same, because only three cipher text variables C_1, C_2 and C_3 are being sent at the encryption side.

Communication Overhead. We observed that the communication overhead is slightly lower than that in [26] at the group key agreement stage, since no certificates are required. In [26], signature is computed over $n + 4$ parameters, but, in proposed one signature is computed on one parameter x_i.

Storage Overhead. Our protocol requires less storage. In [26] protocols each user requires a storage area of $n + 4$ for system parameters, a group encryption, decryption keys and private key. However, our protocol requires only ten storage locations to store the variable P, group encryption and private decryption key.

Simulation. A desktop having Intel(R)Core(TM) i5-2400 CPU at 3·10GHz, frequency 3·09GHz and 2·91GB of RAM is used in evaluating the performance of the proposed protocol. A pairing based cryptography library functions are used in the protocol development, the experimentation is held by varying the number of participants from 2 to 100 by considering the length of group elements in G_1 and G_T is assigned to 171 and 1024 bits respectively. Involvement of exponentiation and multiplication in [13, 18] protocols results more computation time compared to other two protocol. Hence, time cost comparison is done between [26] and proposed protocols (See Table 2.

Figure 1 shows the relationship between the number of group participants and the time required to generate the group encryption key for sender and a participant. From the figure, the time needed by the sender and a participant to generate a group encryption key are almost same and raise linearly as the number of participants increases. However, the cost of time is not high when the number of participants is 100. The [26] protocol consumes 500ms and 495.34ms for the sender and for a participant respectively, where as the proposed protocol needs 502ms and 496.97ms for the sender and for a participant respectively. Figure 2 shows the relationship between the number of group participants and the running time required to generate a group decryption key in both [26] and proposed protocols. From the figure, one can observe that the time cost to generate a group decryption key is increasing linearly with the number of participants. The time cost is ranges from 0.44ms to 132.244ms in [26], where as proposed protocol cost ranging from 0.46ms to 136.523ms. Figure 3 & Figure 4, shows the time cost to generate the ciphertext and decrypt a ciphertext in both the protocols, from figure one can see that time cost is constant irrespective of the number of group participants. The [26] protocol consumes 6.6ms and 6.8ms respectively towards encryption and decryption process. But, the proposed one needs 6.6ms and 6.9ms. Finally, the proposed protocol is consuming almost same time cost as in [26] protocol.

6 Conclusion

We have defined a one round identity based authenticated asymmetric group key agreement protocol from Bilinear maps. The protocol allows the participants in the group to derive a common encryption key, offers the key security and unknown key share properties. Evaluation shows that, the overheads of the proposed protocol are less when compared to others [13, 18, 26]. Computation cost for group common encryption and decryption key generation, ciphertext generation and plaintext extraction is almost same as [26]. Based on our authenticated asymmetric group key agreement protocol,a broadcast based encryption system was proposed. Also, batch multi-signature can be separated into individual signature.

Acknowledgments

The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] A. Abdel-Hafez, A. Miri, and L. O. Barbosa, "Authenticated group key agreement protocols for ad hoc wireless networks," *International Journal of Network Security*, vol. 4, no. 1, pp. 90–98, 2007.

[2] M. J. Bohio and A. Miri, "Self-healing group key distribution," *International Journal of Network Security*, vol. 1, no. 2, pp. 110–117, 2005.

[3] D. Boneh, X. Boyen, and E. Goh, "Hierarchical identity based encryption with constant size ciphertext.," in *EUROCRYPT'05*, LNCS 3494, pp. 440–456, 2005.

[4] E. Bresson, O. Chevassut, and D. Pointcheval, "Dynamic group diffie hellman key exchange under standard assuptoions," in *Proceedings of EUROCRYPT'02*, LNCS 2332, pp. 321–336, 2002.

[5] E. Bresson, O. Chevassut, and J. Quisquater, D. Pointcheval, "Provably authenticated group Diffie-Hellman key exchange," in *Proceedings of ACM CCS'01*, pp. 255–264, 2001.

[6] E. Bresson, O. Chevassut, and J. Quisquater, D. Pointcheval, "Provably authenticated group Diffie-Hellman key exchange," in *Proceedings of AASIACRYPT'01*, LNCS 2248, pp. 290–309, 2001.

[7] M. Burmester and Y. Desmedt, "A secure and efficient conference key distribution system," in *Proceedings of EUROCRYPT'94*, LNCS 950, pp. 275–286, 1995.

[8] J. Camenish, S. Hohenberger, and M. Pedersen, "Batch verification of short signatures," in *Proceedings of EUROCRYPT'07*, LNCS 4515, pp. 246–263, 2007.

[9] X. Cao, W. Kou, and X. Du, "A pairing free identity-based authenticated key agreement protocol with minimal message exchanges," *Information Science*, vol. 180, no. 15, pp. 2895–2903, 2010.

[10] T. Y. Chang, M. S. Hawng, and W. P. Yang, "A communication efficient three party password authenticated key exchange protocol," *Information Science*, vol. 181, no. 1, pp. 217–226, 2011.

[11] K. Y. Choi, J. Y. Hwang, and D. H. Lee, "Efficient ID-based group key agreement with bilinear maps," in *Proceeding of Public Key Cryptography (PKC'04)*, LNCS 2947, pp. 130–144, 2004.

[12] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[13] R. Dutta and R. Barua, "Constant round dynamic group key agreement," in *Proceedings of ISC'05*, LNCS 3650, pp. 74–88, 2005.

[14] R. Dutta and R. Barua, "Password-based encrypted group key agreement," *International Journal of Network Security*, vol. 3, no. 1, pp. 23–34, 2006.

[15] H. Guo, Z. Li, Y. Mu, and X. Zhang, "Provably secure identity based authenticated key agreement protocols with malicious private key generators," *Information Science*, vol. 181, no. 3, pp. 628–647, 2011.

[16] S. Hong, "Queue-based group key agreement protocol," *International Journal of Network Security*, vol. 9, no. 2, pp. 135–142, 2009.

[17] A. Joux, "One round protocol for tripartite diffie-hellman," *Journal of Cryptology*, vol. 17, no. 4, pp. 263–276, 2004.

[18] J. Katz and M. Yung, "Scalable protocols for authenticated group key exchange," in *Proceedings of Crypto'03*, LNCS 2729, pp. 110–125, 2003.

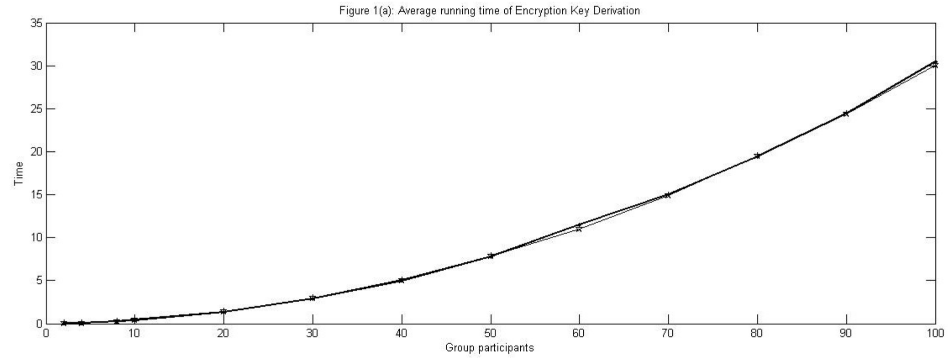

Figure 1: Average running time of encryption key derivation

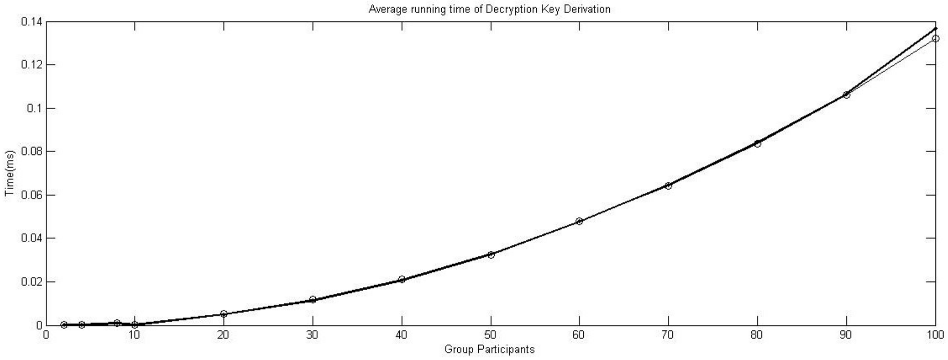

Figure 2: Average running time of decryption Key Derivation

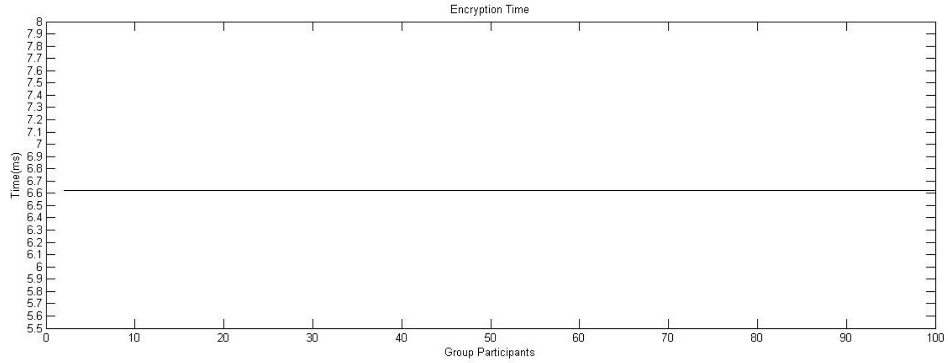

Figure 3: Message encryption time

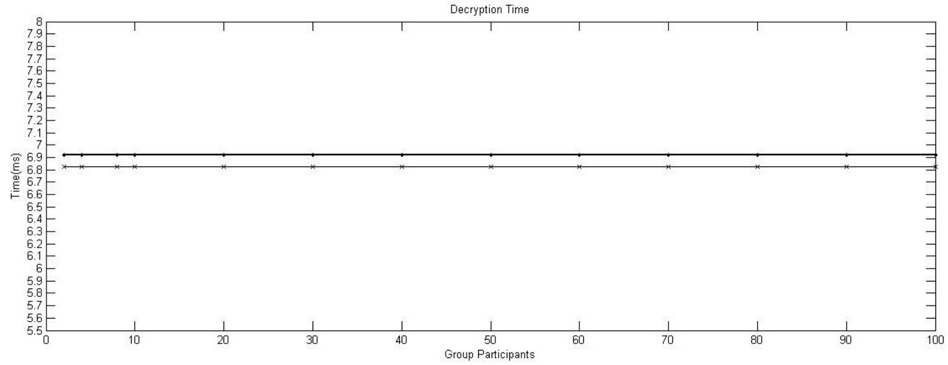

Figure 4: Message decryption time

[19] D. Li and S. Sampalli, "A hybrid group key management protocol for reliable and authenticated rekeying," *International Journal of Network Security*, vol. 6, no. 3, pp. 270–281, 2008.

[20] R. Sivaranjani, D. L. Bhaskari, and P. S. Avadhani, "Current trends in group key management," *International Journals of Advanced Computer Science and Applications*, vol. 2, pp. 82–86, 2011.

[21] A. Shamir, "Identity based cryptosystem and signature schemes," in *Advances in Cryptology (Crypto'84)*, LNCS 196, pp. 47–53, 1984.

[22] R. Srinivasan, V. Vaidehi, R. Rajaraman, S. Kanagaraj, R. C. Kalimuthu, and R. Dharmaraj, "Secure group key management scheme for multicast networks," *International Journal of Network Security*, vol. 11, no. 1, pp. 33–38, 2010.

[23] Q. Wu, Y. Mu, W. Susilo, B. Qin, and J. Domingo-Ferrer, "Asymmetric group key agreement," in *Proceedings of EUROCRYPT'09*, LNCS 5479, pp. 153–170, 2009.

[24] Q. Wu, Y. Mu, W. Susilo, B. Qin, and J. Domingo-Ferrer, "Provably secure one-round identity based authenticated asymmetric group key agreement protocol," *Information Sciences*, vol. 181, no. 19, pp. 4318–4329, 2011.

[25] L. Zhang, B. Qin, Q. Wu, and F. Zhang, "Efficient many-to-one authentication with certificateless aggregate signatures," *Computer Networks*, vol. 54, no. 14, pp. 2482–2491, 2010.

[26] L. Zhang, Q. Wu, U. G. Nicolas, B. Qin, and J. Domingo-Ferrer, "Asymmetric group key agreement protocol for open networks and its application to broadcast encryption," *Computer Networks*, vol. 55, no. 15, pp. 3246–3255, 2011.

[27] L. Zhang, F. Zhang, Q. Wu, and J. Domingo-Ferrer, "Simulatable certificateless two party authenticated key agreement protocol information," *Information Science*, vol. 180, no. 6, pp. 1020–1030, 2010.

Reddi Siva Ranjani is a research scholar in Andhra University under the supervision of Prof.P.S.Avadhani and Prof.D.Lalitha Bhaskari in Computer Science and Systems Engineering. She received her M.Tech (CSE) from Andhra University and presently working as Associate Professor in CSE Department of GMRIT. She is a Life Member of ISTE. Her research areas include Network Security, Cryptography, Group Key Management.

D. Lalitha Bhaskari is an Professor & HOD in the department of Computer Engineering, Andhra University college of Engineering for women . She is guiding more than 8 Ph. D Scholars from various institutes. Her areas of interest include Theory of computation, Data Security, Image Processing, Data communications, Pattern Recognition. She is a Life Member of CSI and CRSI. Apart from her regular academic activities she holds prestigious responsibilities like Associate Member in the Institute of Engineers, Associate Member in the Pentagram Research Foundation, Hyderabad, India. She also received young engineer award from Institute of Engineers (India) in the year 2008.

P. S. Avadhani is a Professor in the department of Computer Science and Systems Engineering and Vice Principal of AU College of Engineering, Andhra University. He has guided 10 Ph. D students and right now he is guiding 12 Ph. D Scholars. He has guided more than 100 M.Tech. Projects. He received many honors like best researcher award and best academician award from Andhra University, chapter patron award from CSI for CSI-Visakhapatnam Chapter and he has been the member for many expert committees, member of Board of Studies for various universities, Resource person for various organizations. He has coauthored 4 books. He is a Life Member in CSI, AMTI, ISIAM, ISTE, YHAI and in the International Society on Education Technology.